# Trust based Data Plane Security Mechanism for a Mobile Ad hoc Network through Acknowledgement Reports

Shirina Samreen
Research Scholar, Dept. of Computer Science
JNTUH College of Engineering
Kukatpally, Hyderabad, A.P., India

G. Narsimha, PhD
Associate Prof., Dept. of Computer Science
JNTUH College of Engineering
Nachupally, Kondagattu, Karimnagar, A.P., India

## ABSTRACT
Malicious packet drop attack over the data plane in a MANET involves malicious nodes dropping the data packets after the route formation. In this paper, a security mechanism has been proposed to detect those nodes which exhibit the malicious behavior by dropping the data packets during the data transmission phase after participating in the route establishment phase without exhibiting any malicious behavior. The detection is done based upon a trust management framework employing the Dempster Shafer Theory to represent the trust. The design of the trust management framework has been covered in earlier works and the current work focuses upon its application for the design of a novel security mechanism. Trust is computed based upon the forwarding behavior represented by acknowledgement reports submitted to the source node. The composition of the report ensures that the source node can verify its authenticity. Trust updates upon intermediate nodes are done by the source node at the end of a session which facilitates the secure route formation through the proposed mechanism. The efficiency and accuracy of the proposed security mechanism is validated using the network simulator ns2 and the experimental results show that the proposed mechanism outperforms the other schemes.

## General Terms
Mobile Ad hoc Networks, Data Plane Security.

## Keywords
Acknowledgement Reports, Packet Droppers, Trust Management Framework, Reward Factor, Punishment Factor.

## 1. INTRODUCTION
Malicious packet dropping in a MANET occurs when a node has been compromised by an adversary and intends to disrupt the network performance by simply dropping the packets without forwarding them.

A security mechanism known as Anti Black hole mechanism addresses packet dropping at the control plane is proposed in [1] wherein the adversary drops the data packets after forcibly acquiring a route by manipulating the sequence number and hop count values of the routing packets. But the approach requires the deployment of special IDS (Intrusion Detection System) nodes which perform the promiscuous neighborhood monitoring to determine the difference between the number of RREQ packet and the number of RREP packets forwarded by a node to assign it a suspicious value based upon which it is declared as malicious node. The main drawback of the proposed scheme is that it requires the deployment of IDS nodes. An approach for the detection of malicious packet dropping at the data plane is proposed in [2]. It employs IDS nodes which are trusted and turn into promiscuous mode for monitoring the data forwarding activity upon the detection of malicious behavior. The approach has the following limitations:

- It requires special IDS nodes which are assumed to be always trusted. In an open environment like MANET, it is very difficult for any node to remain trusted for a long time as the probability of a node being compromised by an adversary is inevitable.
- Usage of promiscuous mode is more energy consuming and the drawback of false alarms in case of receiver collisions and ambiguous collisions.
- It also has the requirement about the placement of IDS nodes that each IDS node should always be a neighbor to some other IDS node. In a mobile ad hoc network, this implies that the IDS nodes have a restricted mobility.
- The attack discovery is based upon the probing done by the destination node with each of the intermediate nodes which respond with a count of number of data packets forwarded. Usage of a simple count of the forwarded data packets is always prone to manipulation since the destination cannot verify the authenticity.
- The paper does not describe about the handling of link breaks by the attack discovery process.

The proposed security mechanism aims to provide the detection and isolation of malicious packet droppers so as to overcome the limitations in the approach proposed in [2].

- Firstly, it does not need any special trusted IDS nodes.
- Secondly it employs an acknowledgement based approach rather than promiscuous monitoring so as to conserve the energy of the nodes. The control overhead associated with acknowledgement based approaches is reduced by having a session based acknowledgment report rather than per-packet acknowledgement.
- Thirdly it employs a trust model based upon Dempster Shafer theory to compute the subjective trust by the source node and the trust model facilitates the composition of malicious list.
- Fourthly, the detection of malicious behavior is done through acknowledgement reports which are composed such that the authenticity of the report can be verified by the source node.
- Lastly, the proposed mechanism has a clearly defined way of dealing with link breaks which

ensures that the malicious node cannot be obscured from detection.

The paper is organized as follows. Section 2 presents the related work, section 3 gives the details of the proposed security mechanism, section 4 presents the performance analysis through experimental results and section 5 presents the conclusion and future work.

## 2. RELATED WORK

Packet dropping attack which involves an adversary dropping the packet in such a way that it evades detection and can cause a legitimate node to come under suspicion is termed as Stealthy Packet Dropping Attack [3]. This attack can be countered by having two additional requirements over baseline monitoring of having the neighbors maintain additional information about the routing path and to have some additional checking responsibility to each neighbor.

An approach which provides a resource efficient accountability for node misbehavior in MANET based upon random audits is the REAct system [4]. It can be used to locate individual misbehaving nodes that perform packet drop attack. It uses bloom filters as node behavioral proofs for the forwarding activity but it fails under colluding adversarial model.

An acknowledgement based scheme is in [5], the source node expects acknowledgements from the destination as well as the intermediate nodes. Based upon the missing acknowledgements, the neighborhood nodes are required to promiscuously monitor the forwarding activity to detect the packet droppers. A drawback of the technique is that a lot of network traffic is created in the form of acknowledgement packets. A secure on-demand routing protocol used to detect faults in the source to destination path which may include nodes dropping or modifying the packets is proposed in [6] named as Robust Source Routing (RSR) which provides data origin authentication services and integrity checks. The main drawback of the proposed scheme is that it heavily relies upon public key cryptography and also having an ACK sent to the destination for each data packet adds up to the control overhead.

## 3. PROPOSED SECURITY MECHANISM

The proposed security mechanism leverages upon a trust management framework which has been covered in earlier works [7] for the detection of malicious packet droppers which target the data plane security by behaving honestly during route formation and exhibit the malicious behavior during data transmission by simply dropping the packets. The current paper focuses upon the application of trust management framework in the design of a novel security mechanism for secure data transmission. The impact of various parameters upon the performance of the proposed security mechanism has been analyzed by varying the values of each of these parameters. Two of these parameters are related to the trust management framework which includes the reward factor and punishment factor and another parameter related to the proposed security mechanism which is the number of packets transmitted during a session.

Malicious packet droppers during the current communication session are identified and this information is utilized for the establishment of secure routes for the future communication sessions. This is accomplished by eliminating the malicious packet droppers which have been detected in the past communication sessions from the routes during the route establishment. It consists of five phases which are described below.

Each communication session comprises of the transmission of N (fixed value) packets. In the Data Transmission phase, the source node transmits N packets and each intermediate node sends a link layer acknowledgement to its upstream neighbor. The link layer acknowledgement comprises of a pre-computed hash value unique for each packet which is used to compose the acknowledgement report. After the transmission of N packets, the source node enters into the Reports Request phase which results in the reception of acknowledgement reports from each of the intermediate nodes. This is followed by the Reports Processing phase which involves the analysis of the received reports to detect the malicious packet droppers which are blacklisted. The Blacklist Propagation phase involves the broadcasting of the blacklisted nodes so as to alert the other nodes in order eliminate them from participating in any of the routes. The Secure Route Establishment phase uses the information from the Blacklist Propagation phase to eliminate the blacklisted nodes from the future routes. The distribution of certain pre-computed hash values to each of the intermediate nodes on the path by the destination node which are used to form the acknowledgement reports is also done in the Secure Route Establishment phase.

### 3.1 Trust Management Framework

The details of the design of trust management framework (TMF) have been covered in earlier works [7]. It involves a mapping of the variables (α, β) of the beta probability distribution to the tuple (b, d, u) representing belief, disbelief and uncertainty respectively for the explicit quantification of uncertainty. Each session ends with an update of variables α and β representing a measure of cooperative and malicious behavior respectively. Periodic updates of α and β involve factors called as reward and punishment factors represented by γ and μ respectively.

$$\alpha(t+1) = \alpha(t) \times \tau_p(t) + p \qquad \beta(t+1) = \beta(t) \times \tau_q(t) + q$$

$$\tau_p(t) = \gamma \times \frac{\alpha(t)}{\alpha(t)+1} \qquad \tau_q(t) = \mu \times \frac{\beta(t)}{\beta(t)+1}$$

The above equations represent the periodic updates involving the reward factor and punishment factor.

### 3.2 Secure Route Establishment

The source node broadcasts the RREQ packet which contains an additional field of a random value r encrypted using the secret key shared with the destination node. This random value is used by the destination to generate certain values which have to be distributed to each of these intermediate nodes. Each of the intermediate nodes on the path uses these values to compute a value which acts an acknowledgement for each of the received packet which has to be sent to the upstream node on the path. The received acknowledgement values have to be incorporated within the acknowledgement report by each of the intermediate nodes as a proof of the packet forwarding activity.

Upon receiving an RREQ packet, a node checks whether the node from whom the packet is received exists in its blacklist. Under these circumstances, the RREQ packet is dropped. Otherwise, it is forwarded and further broadcasted. The destination node maintains a list known as alert list pairs which contains the pairs of nodes (x, y) such that the source to

destination path should not have node x and node y as successive nodes. The alert list pairs are determined by the source node as a result of reports analysis done in the Reports Processing phase. Upon receiving the RREQ packet, the destination node first checks whether the route formed so far involves any pair of successive nodes which fall into the category of alert list pairs. Under these circumstances, the RREQ packet is dropped; otherwise the RREP packet is formed and sent back towards the source node.

The formation of the RREP packet by the destination node is preceded by the following: The random value r in the RREQ packet is decrypted and the hash values $h^k(r)$, $h^{k-1}(r)$, …. , $h^2(r)$, h(r) are computed which are sent to the intermediate nodes 1, 2, 3,…., k respectively by encrypting them with the secret keys shared by destination with each of these intermediate nodes. In other words, the values $E(K_{S1}, h^k(r))$, $E(K_{S2}, h^{k-1}(r))$, …., $E(K_{Sk}, h(r))$ are incorporated into the RREP packet where $K_{S1}$, $K_{S2}$, $K_{S3}$, ..... , $K_{Sk}$ are the symmetric keys which the destination shares with the intermediate nodes 1, 2, 3, …., k respectively.

## 3.3 Data Transmission

After the completion of the Secure Route Establishment phase, the source node gets into the Data Transmission phase which takes place in successive communication sessions. Each communication session comprises of sending N packets and waiting for fixed duration of time which is the time required for the transmission of N packets from the source to destination by traversing through k hops where k is the length of the route that has been established.

Each intermediate node on the path has to compose an acknowledgement report for each communication session in which it participates. The report comprises of an N-bit flag (initialized to all zeros) and a set of N acknowledgement values (initialized to zeros). The N-bit flag is used to indicate those packets which have been received by a node during a communication session comprising of N packets. If a packet with sequence number i (0<=i<=N), has been received by a node, then the $i^{th}$ bit position is set to 1. The set of N acknowledgement values within the report for each of the packets that have been forwarded to it's downstream node act as proof of the forwarding activity and are received in the form of ACK packets from it's downstream node on the source to destination path. Hence the acknowledgement report can be used to locate those packets which have been received by a node from its upstream neighbor but have not been forwarded to its downstream neighbor by looking for those bit positions in the N-bit flag with a 1 value and a missing / incorrect acknowledgement value.

The acknowledgement values for each of the received packets are computed by the intermediate node and sent to its upstream neighbor. The computation is done using the pre-computed hash value obtained during the Secure Route Establishment phase for the ongoing communication session. The hash is computed over the concatenation of packet id of the received packet and the hash obtained during the Secure Route Establishment. For example, if an intermediate node p receives a packet with packet id X, then the acknowledgement value is computed as follows:

$$h(X \parallel h^{k-p+1}(r))$$

Where k is the number of intermediate nodes and r is the encrypted random value sent by the source to the destination in the RREQ packet and $h^{k-p+1}(r)$ is the pre-computed hash value obtained through RREP from the destination node.

The destination node also composes the acknowledgement report but it consists of only the N-bit flag as the destination node does not have any upstream neighbor for the reception of acknowledgement values. The node upstream to the destination node also does not have any acknowledgement value as the N-bit flag of the destination node itself acts a proof of the forwarding activity since the destination node is assumed to be trusted by the source.

In a network topology with the source to destination path as (S, A, B, C, E, F, G, D) with each session comprising of 5 packets (N=5), assume that a link break occurs at link C-E at the data packet with the sequence no. 3 and the RERR packet sent by C reaches source node S after transmission of data packet with the sequence no. 4. The acknowledgement reports from each of the intermediate nodes on the source to destination path are depicted in Fig. 4 where u1, u2, u3 and u4 are the packet ids'.

## 3.4 Reports Request

After the successful completion of sending out N packets upon the outgoing interface, the source node enters into the Reports Request phase which is carried on in two different ways based upon two possible cases:

Case 1: No link break has occurred and hence the existing route from the source to destination can be used to request for acknowledgement reports from each of the intermediate nodes and the destination node. The source node creates a CLEAR packet which causes all the intermediate nodes and the destination node to send the reports.

Case 2: A link break has occurred and hence the existing source to destination route cannot be used. Hence the source node creates a RPTRQ packet (Reports Request) which contains the identities of the nodes which formed the path. The RPTRQ packet is broadcast similar to RREQ packet throughout the network. The processing of the RPTRQ packet is done in two parts which causes each intermediate node to update the routing table for reaching the source and also sending of the REPORT packet on the reverse path. The reception of the REPORT packet from the destination serves the dual purpose of route establishment as well as the report reception.

In the former case, the source node unicasts the CLEAR packet along the same path to the destination, which causes all the intermediate nodes and the destination node, send the REPORT packets along the reverse path. In the latter case, the source node broadcasts the RPTRQ packets and each of the intermediate nodes and the destination node send their REPORT packets along the reverse of the path along which the RPTRQ packet was received.

## 3.5 Reports Processing

The source node upon receiving the REPORT packets from all of the intermediate nodes and also the destination node enters into the Reports Processing phase. Firstly, the report from the destination node is analyzed and count of the number of bit positions with a 0 in the N-bit flag are checked to see if it is less than 20% of the number of packets sent. The above condition indicates that no malicious node exists in the source to destination path and the same path can be used.

Otherwise, the source node composes two lists namely: suspicious list and malicious list (or blacklist). The suspicious list consists of those nodes which exhibited misbehavior along with their occurrence counts whereas the malicious list consists of those nodes which have been detected as malicious

based upon their occurrence counts in the suspicious list. The REPORT packets received from each of the intermediate nodes and the destination node are analyzed to check for one of the following conditions: If the REPORT packets of all the nodes have the N-bit flags as all zeros, then it indicates that first node in the set of intermediate nodes has to be included in the suspicious list. Otherwise, for each intermediate node x, the source node examines the N-bit flag in the REPORT packet and for each bit position i (0<i<N+1) having a value 1, it computes the acknowledgement value for each of the packets with sequence number i as $h(i \parallel h^{k-x+1}(r))$ where r is the random value which the source sent to destination in the RREQ, k is the number of intermediate nodes. The presence of the correct acknowledgement value in the REPORT packet proves the fact that node x has indeed forwarded the packet i to its downstream node x+1.

The following counts are made to perform the trust updates of each intermediate node and compose the suspicious list and malicious list:

- Count of the number of bit positions with a 1 in the N-bit flag (say NR) representing the number of packets received from its upstream node which have to be forwarded to the downstream node.
- Count of the number of bit positions with a 1 in the N-bit flag along with correct acknowledgement value (which indicates number of packets correctly forwarded downstream, say NF)
- Count of the number of bit positions with a 1 in the N-bit flag and a missing/incorrect in the acknowledgement report (which indicates number of packets dropped without forwarding, say ND)
- If the ratio NR/ND is greater than 0.2, then the two successive nodes x and x+1 are equally likely to be malicious.

### *3.5.1 Trust Update*

For each intermediate node, the value of NF represents the value of p, which is the number of cooperative behaviors within the session and the value of ND is used to compute the value of q representing the number of malicious behaviors. If the node i does not have a correct acknowledgement value for a packet, it is equally likely that both the nodes i and i+1 are malicious. Hence both nodes i and i+1 have to be penalized but the penalization is in proportion to the neighboring nodes trust. In other words,

p(i) = NF, q(i) = ND x Trust(i+1) and q(i+1)=ND x Trust(i)

The values of p and q for the current communication session update the values of α and β which is followed by the update of the tuple (b, d, u) thereby updating the trust at the end of reports processing.

### *3.5.2 Composition of Alert list pairs, Suspicious and Malicious list*

After the trust update, the pairs of intermediate nodes on the path <i, i+1> which satisfy the condition that NR(i) / ND(i) is greater than 0.2, then both nodes i and i+1 have to be considered for composing the suspicious list. The conclusion of which of the two nodes from i and i+1 is more likely to be malicious is done based upon the trust value associated with each node. Out of the two nodes i and i+1, the one with a lesser trust is included in the suspicious list. If both have equal trust, then both are included. Periodically, the suspicious list is scanned to check the nodes with the occurrence count greater than MAL_THRESH (maximum number of times a node can exhibit suspicious behavior). All such nodes are moved into malicious list. If the nodes i and i+1 have equal trust, then such a pair of successive nodes <i, i+1> are termed as alert list pairs which is provided to the destination in the RREQ packet for the next communication session so as to avoid any route with <i, i+1> as successive nodes for the next session.

After the analysis of the reports and the composition of suspicious list, malicious list and alert list pairs, the source node has to initiate the next successive communication session (if it has any more packets to be transmitted). A fresh route from source to destination is formed which does not involve any nodes in the malicious list and any successive nodes on the path from the alert list pairs. The propagation of information about the malicious list is carried on by the Blacklist Propagation phase and the information about alert list pairs is incorporated by the source node in the RREQ packet in the Secure Route Establishment phase.

## 3.6 Blacklist Propagation

The nodes included into the malicious list are termed as blacklisted nodes and this information has to be propagated in the network through MALI packet which contains the list of nodes included into the malicious list. All the nodes in the network update their blacklist through the MALI packet which is used during secure route establishment.

| NID | N-bit flag | Ack values of each of the N pkts transmitted within a session (N=5) | | | | |
|---|---|---|---|---|---|---|
| | | Ack val of pkt1 | Ack val of pkt2 | Ack val of pkt3 | Ack val of pkt4 | Ack val of pkt5 |
| A | 11110 | $h(h^5(r)\|\|u1)$ | $h(h^5(r)\|\|u2)$ | $h(h^5(r)\|\|u3)$ | $h(h^5(r)\|\|u4)$ | 0 |
| B | 11110 | $h(h^4(r)\|\|u1)$ | $h(h^4(r)\|\|u2)$ | $h(h^4(r)\|\|u3)$ | $h(h^4(r)\|\|u4)$ | 0 |
| C | 11110 | $h(h^3(r)\|\|u1)$ | $h(h^3(r)\|\|u2)$ | $h(h^3(r)\|\|u3)$ | $h(h^3(r)\|\|u4)$ | 0 |
| E | 11000 | $h(h^2(r)\|\|u1)$ | $h(h^2(r)\|\|u2)$ | 0 | 0 | 0 |
| F | 11000 | $h(h(r)\|\|u1)$ | $h(h(r)\|\|u2)$ | 0 | 0 | 0 |
| G | 11000 | No ack values needed since the node is the immediate upstream to destination node | | | | |
| D | 11000 | No ack values needed as the node is the destination node | | | | |

**Fig. 4. Acknowledgement reports for a session**

# 4. PERFORMANCE ANALYSIS

The performance analysis of the proposed technique against the varying number of malicious nodes is done using the ns2 network simulator. An area of 800m x 800m, and 50 nodes executing the proposed security mechanism with the AODV routing protocol (modified AODV or MAODV) were randomly distributed out of which few nodes act as malicious nodes performing the black hole attack. Ten pairs were randomly chosen for data transmission, each sending 6kb UDP-CBR (Constant Bit Rate) per second. All the nodes (the normal nodes as well as malicious nodes) move in a Random-way point mobility model.

**Table 1.Experimental Parameters**

| Parameter | Value |
|---|---|
| Coverage area | 800m X 800m |
| Number of nodes | 50 |

| | |
|---|---|
| Transmission range | 150 m |
| Simulation time | 1000 s |
| Mobility | Random way point model |
| Traffic type | UDP – CBR (Constant Bit Rate) |
| Packet size | 512 bytes |
| Maximum speed | 0m/s, 10m/s, 20m/s, 30m/s, 40m/s, 50m/s |
| Pause time | 1 s |

m = meter, s = second

The parameters of the ns2 experimental data are listed in Table I and the each data value refers to an average value computed through 20 experiments. The performance evaluation comprises of the comparison with Anti-Black hole mechanism(ABM) and the Modified DSR(MDSR) schemes since the proposed approach intends to overcome the limitations of the approaches proposed in MDSR. An average of 20 experiments under different random movement scenarios is considered for each point in each of the graphs. The following metrics are considered for performance evaluation.

***Packet Delivery Fraction (PDF)*** is computed as the ratio of total number of packets received by the destination to the total number of packets sent by the source node.

***Routing Overhead (ROV)*** is defined as the percentage of control packets which form the total traffic comprising of data packets and control packets.

***Average end-to-end delay*** is defined as the average time taken for data packets to reach the destination node from the source node.

***Detection ratio*** is the ratio of the number of nodes whose behavior (malicious or non-malicious) is identified correctly to the actual number of such nodes in the network.

***False Positive Ratio*** is defined as the ratio of the total number of false positives to the total number of normal (non-malicious) nodes multiplied by 100 where a false positive is defined as a normal node being falsely detected as a malicious node.

***False Negative Ratio*** is defined as ratio of the total number of false negatives to the total number of malicious nodes multiplied by 100 where a false negative is defined as a malicious node being falsely detected as a non-malicious node.

**Experiment 1: Varying the value of γ (keeping μ as constant set to 0.6) and varying the value of μ (keeping γ as constant set to 0.4)**

The purpose behind the experiment is to analyze the effect of change in the values of γ (reward factor) and μ (Punishment factor) which contribute to the timed-based aging factors of the variables α and β within the trust model which in turn affects the efficiency of the proposed scheme in the detection of malicious packet droppers. The metrics used to illustrate the effect on efficiency are detection ratio, false positive ratio and false negative ratios.

Firstly, the value of γ is varied keeping the value of μ as constant (set to 0.6) and secondly the value of μ is varied keeping the value of γ as constant (set to 0.4). Fig. 5(a) shows that the value of 0.4 for γ has the highest detection ratio (with μ set to 0.6) and for values less than 0.4 or greater than 0.4 the detection ratio is lesser. For values less than 0.4, as the value of γ increases (smaller proportion of good behavior in the past is considered to update current value of the trust metric), the false positives decrease since the cooperative behaviors over longer periods of time are required to substantially increase the value of α. For values greater than 0.4, as the value of γ increases (larger proportion of good behavior in the past is considered to update the current value of the trust metric), the number of false negatives increase since the cooperative behaviors over shorter periods of time are required to substantially increase the value of α which may cause many malicious nodes to obscure from detection.

Fig. 5(b) shows that the value of 0.6 for μ has the highest detection ratio (with γ set to 0.4) and for values less than 0.6 or greater than 0.6 the detection ratio is lesser. For values less than 0.6, as the value of μ increases (smaller proportion of bad behavior in the past is considered to update the current value of the trust metric), the false negatives ratio increases since the uncooperative behaviors over longer periods of time are required to substantially increase the value of β. For values greater than 0.6, as the value of μ increases (larger proportion of bad behavior in the past is considered to update the current value of the trust metric), the false positives ratio increases since the uncooperative behaviors over shorter periods of time are required to substantially increase the value of β which may cause many non-malicious nodes to be wrongly detected as malicious. Hence from the experimental analysis, it can be observed that the values of γ=0.4 and μ=0.6 gives the highest detection ratio.

**Experiment 2: Effect of the parameter N (number of packets per communication session) on the performance**

The value of N determines the memory to be allocated for the report packets. Hence a very large value may not be feasible in a resource constrained environment like MANET. Through the experimental analysis, it was found that N<=50 would execute the protocol without any memory issues. The impact of N upon the execution of the protocol is illustrated through an experiment which shows the impact of N upon the Packet delivery fraction, Routing Overhead and Average end-to-end delay with varying speed and varying values of N (10, 30, 50).

As can be observed from Fig. 6(a), for all values of N, (N=10, 30 and 50) the PDF decreases as the speed increases since the number of link breaks increase and hence route establishment occurs frequently. The average PDF is highest with N=50 as 85.435% compared to 85.116% and 80.5% obtained with N=30 and N=10 respectively. For all the experiments the number of malicious nodes is considered to be 10. As the value of N is smaller, the data transmission is interrupted by the reports processing phase thereby resulting in an increase in the queuing delay which may result in some packet drops if the queue is full and hence a decreased PDF happens with N=30 and N=10.

From the Fig. 6(b), it can be observed that , for all values of N, (N=10, 30, 50) the ROV increases as the speed increases since the number of link breaks increase and hence route establishment occurs frequently. The average ROV is highest with N=10 as 0.1766 whereas the ROV is 0.145 and 0.176 with N=50 and N=30 respectively. As the value of N is smaller, the data transmission is interrupted by the reports processing phase thereby resulting in an increase in the number of report packets generated causing an increased routing overhead.

The average end-to-end delay with varying speeds and varying values of N has been shown in Fig. 6(c). For all values of N, (N=10, 30 and 50) the delay increases as the speed increases since the number of link breaks increase and hence route establishment occurs frequently. The average end-to-end delay is highest with N=10 as 61ms compared to 46.83ms and 53.16ms respectively with N=50 and N=30 respectively. As the value of N is smaller, the data transmission is interrupted by the reports processing phase thereby resulting in an increase in the queuing delay which

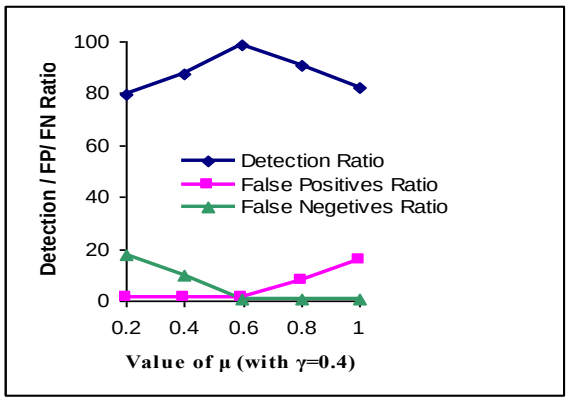


**Fig. 5(a). Effect of γ**

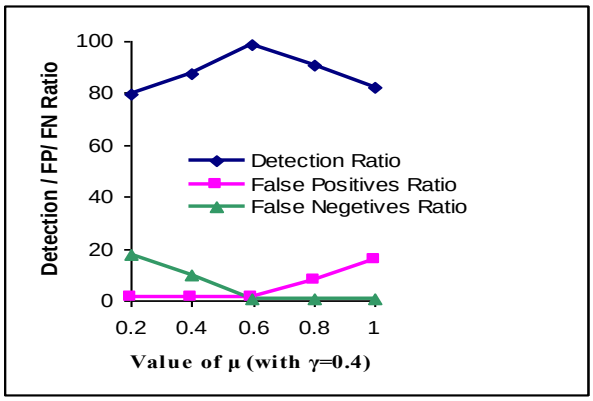


**Fig. 5(b).Effect of μ**

adds up to the average end-to-end delay.

**Experiment 3: Varying the mobility speed with constant number of malicious nodes (set to 10 and N=50)**

Fig. 7(a) shows the change in PDF with varying speeds wherein the first observation is that for all the schemes, the proposed MAODV, MDSR and ABM, the PDF falls down as the speed increases since more and more link breaks may result in an increased packet loss. The average PDF for all speeds is 85.435% with MAODV whereas it is 82.25% and 79.33% with MDSR and ABM respectively.

The increased PDF of the proposed approach is attributed to its efficiency in the accurate detection of malicious packet droppers since it employs an acknowledgement based approach whereas the approaches in ABM and the MDSR are based upon promiscuous mode which is prone to false alarms in case of receiver collisions and ambiguous collisions and fail in the case of an IDS node getting compromised by the adversary.

The change in ROV with varying speeds is shown in Fig. 7(b) wherein the first observation is that for all the schemes, the proposed MAODV, MDSR and ABM, the ROV rises as the speed increases since more and more link breaks may result in more number of control packets for route re-establishment. The average ROV for all speeds is 0.1266 with MAODV whereas it is 0.1616 and 0.185 with MDSR and ABM respectively. The detection mechanism along with the control

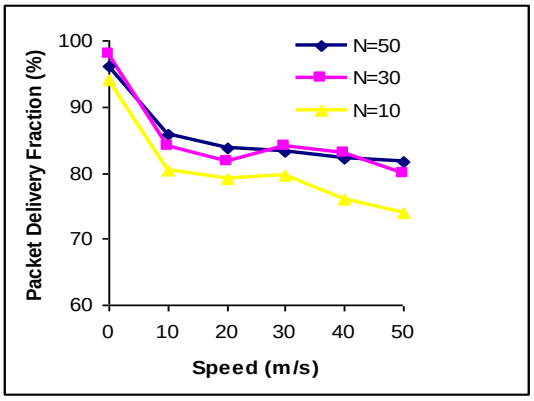


**Fig. 6(a). Packet Delivery Fraction**

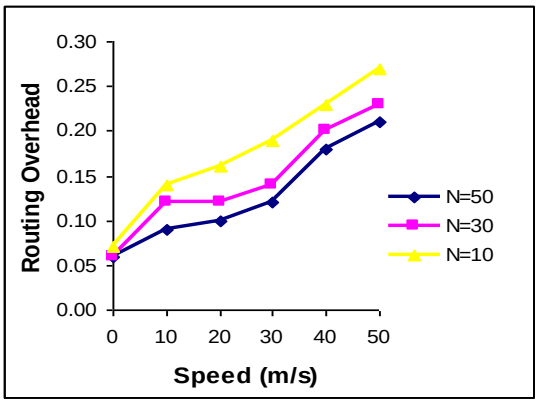


**Fig. 6(b). Routing Overhead**

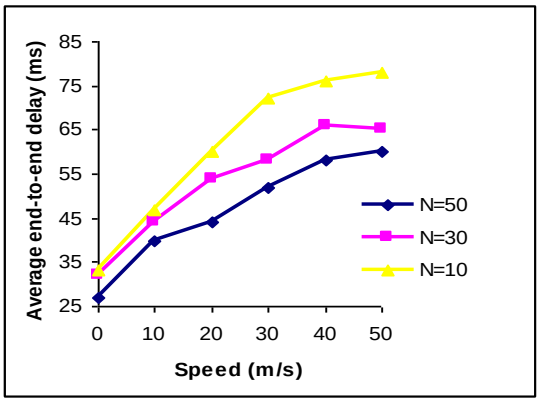


**Fig. 6(c). Average end-to-end delay**

packets used for the detection and isolation of malicious node in MDSR (including QREQ, QREP, MNREQ, and ALARM packets) and ABM incur an increased routing overhead compared to the proposed MAODV approach.

Fig. 7(c) shows that the detection ratio increases with the increase in speed since the number of interactions among the nodes increase with an increase in speed. Due to a trust model based upon uncertainty reasoning with the trust metrics being computed through an acknowledgement based scheme, the average detection ratio of the proposed MAODV is 95.08% which is much better compared to MDSR and ABM with average detection ratios of 91.58% and 86.75% respectively which are based upon the usage of IDS nodes and promiscuous neighborhood monitoring prone to false alarms.

**Experiment 4: Varying the number of malicious nodes**

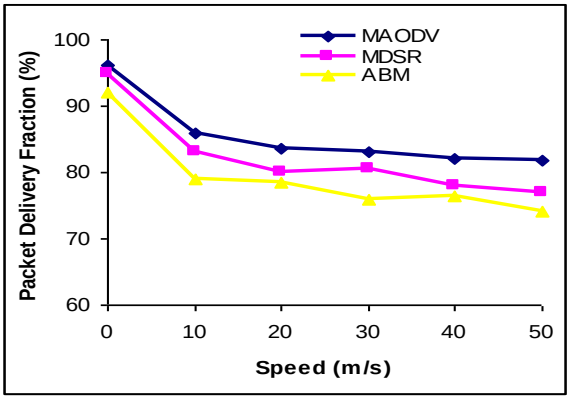


**Fig. 7(a). Packet Delivery Fraction**

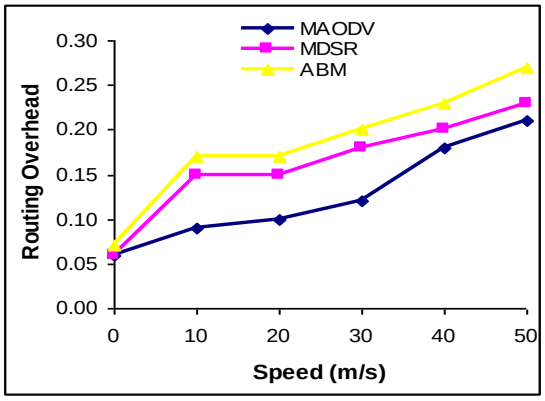


**Fig. 7(b). Routing Overhead**

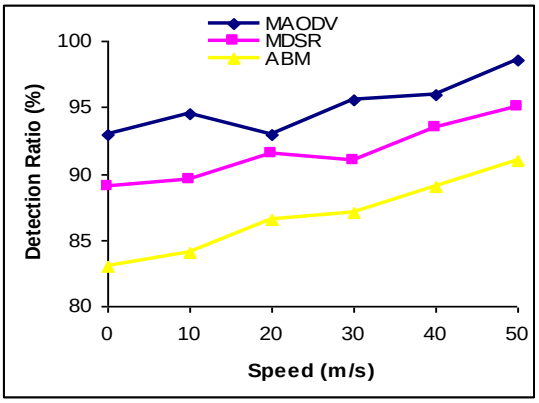


**Fig. 7(c). Detection Ratio**

**with constant mobility speed (set to 50m/s)**

Fig. 8(a) shows the change in PDF with varying number of malicious nodes wherein the first observation is that for all the schemes, the proposed MAODV, MDSR and ABM, the PDF falls down as the number of malicious nodes increase since more and more packet drops occur. The average PDF is 85.804% with MAODV whereas it is 81.86% and 78.04% with MDSR and ABM respectively.

Since the proposed approach employs an acknowledgement based approach along with a uncertainty reasoning based trust model to assess the behavior of other nodes, it is more efficient and accurate in the detection of malicious packet droppers whereas the approaches in ABM and MDSR are based upon promiscuous mode and the usage of an IDS which may fail in case of false alarms, receiver collisions, ambiguous collisions and a compromised IDS node.

The change in ROV with varying number of malicious nodes is shown in Fig. 8(b) wherein the first observation is that for

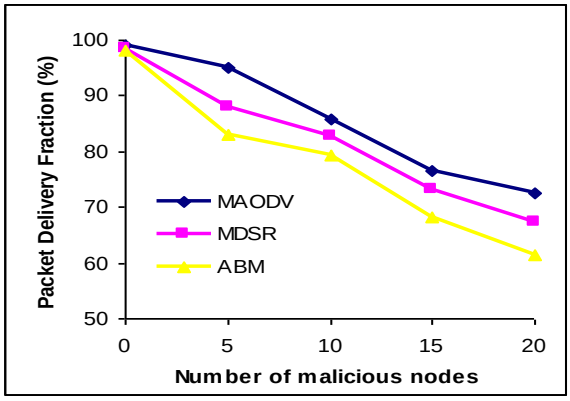


**Fig. 8(a). Packet Delivery Fraction**

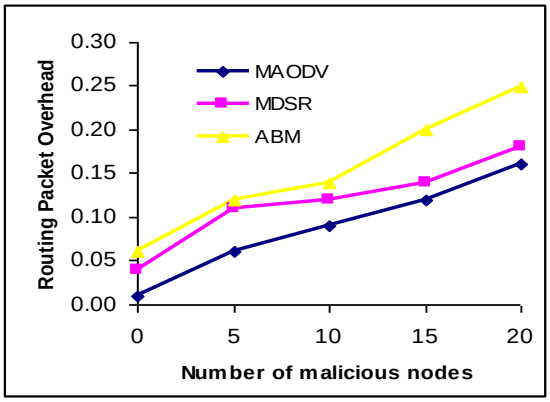


**Fig. 8(b). Routing Overhead**

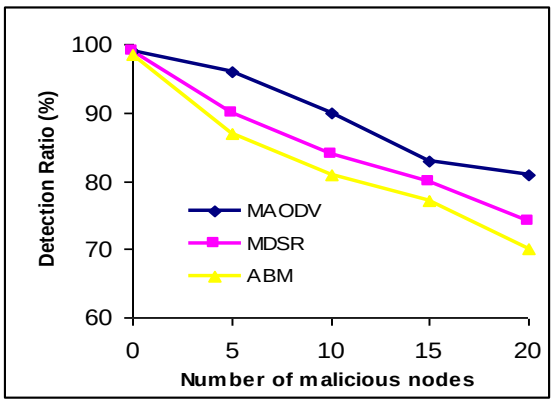


**Fig. 8(c). Detection Ratio**

all the schemes, the proposed MAODV, MDSR and ABM, the ROV rises as the number of malicious nodes increases since the number of control packets involved in the secure route establishment and maintenance increase in the process of detection and isolation of the malicious nodes. The average ROV is 0.088 with MAODV whereas it is 0.118 and 0.154 with MDSR and ABM respectively. The detection mechanism along with the control packets used for the detection and isolation of malicious node in MDSR and ABM incur an increased routing overhead compared to the proposed MAODV approach.

The detection ratio with varying number of malicious nodes is shown in Fig. 8(c) wherein the first observation is, the detection ratio descends with an increase in the number of malicious nodes. The efficiency of the trust model in the proposed MAODV results in an increased detection ratio. With 20 malicious nodes, it has a detection ratio of 81% followed by 74% and 70% for MDSR and ABM respectively.

Since the proposed security mechanism declares a node as malicious after observing its repeated suspicious behavior for a fixed (MAL_THRESH) number of times and moreover it is an acknowledgement based approach unlike the approaches of ABM and MDSR which are based upon promiscuous monitoring prone to false alarms, the proposed mechanism provides a better detection ratios compared to Anti-Black hole Mechanism(ABM) and the Modified DSR(MDSR).

# 5. CONCLUSIONS AND FUTURE WORK

The proposed security mechanism aims to maintain a good packet delivery fraction even in the presence of malicious nodes. This is accomplished by performing the data transmission in the form of successive sessions each comprising of a transmission of a fixed number of packets.

Each session is followed by a reports request phase wherein the source node collects the reports from each of the intermediate nodes and the destination node to perform an analysis based on which the malicious node may be detected. The list of nodes detected as malicious in the current session and the past sessions are specified in the RREQ packet associated with the next successive session so as to eliminate them from the route and maintain a good packet delivery fraction.

The speed with which the detection occurs depends upon a parameter called as MAL_THRESH (set to 2 in the proposed security mechanism) which indicates the maximum number of sessions in which a node can exhibit a suspicious behavior to consider it as malicious behavior. Suspicious behavior is described as a node missing acknowledgement values from its downstream neighbor for more than 20% of the packets received from its upstream neighbor on the path.

If a non-malicious node has a malicious node as its neighbor in more than MAL_THRESH sessions, it may be falsely detected as malicious thereby resulting in an increase in the false positive rate. A malicious node may evade detection by participating in a maximum of MAL_THRESH sessions and having a unique non-malicious node as its neighbor in each session thereby decreasing the true positive rate.

The composition and storage of reports incurs certain memory overhead for each intermediate node on the path and the destination node. The N-bit flag requires N/8 bytes and the 2 byte acknowledgement values for N packets require 2N/8 bytes resulting in total memory storage of 3N/8 bytes. This overhead is justifiable since the overhead is only for the duration of session and the memory is automatically de-allocated after the report submission.

An improvement in the overall packet delivery fraction and the true/false positive ratio (increased true positive ratio and decreased false positive ratio) can be achieved by having an additional mechanism to keep track of the overall good/bad behavior of nodes as exhibited in all the sessions. The future work aims to design a trust framework using the proposed acknowledgement based security mechanism so as to involve each intermediate node as well as the source node in the trust establishment process using direct observations as well as recommendations so as to determine an unbiased reputation rating/trust metric for each intermediate node by every other node based upon the forwarding behavior exhibited over a period of time and dynamically update the trust metric based upon the behavioral changes.

# 6. REFERENCES

[1] Ming-Yang Su. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Comput Commun 2010

[2] M.Mohanapriya, Ilango Krishnamurthi. Modified DSR protocol for detection and removal of selective black hole attack in MANET. Comput and Elec Engg 2013

[3] Khalil And Bagchi: Stealthy Attacks In Wireless Ad Hoc Networks: Detection And Countermeasure, IEEE Trans On Mobile Computing, Vol. 10, No. 8, Aug 2011

[4] W. Kozma, and L. Lazos, "REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits", Second ACM Conference on Wireless Network Security (WiSec), pp. 103-110, 2009

[5] Muhammad Zeshan, et al., "Adding Security against Packet Dropping Attack in Mobile Ad Hoc Networks", Intern Seminar on Future Info Tech and Mgmt Engg, pp. 568- 572, Nov 2008

[6] Crepeau, C., et al., "A secure MANET routing Protocol with resilience against Byzantine behaviors of malicious or selfish nodes". 21st IEEE Inter conf on Adv Info Net and App Workshops AINAW 2007, Canda (2007)

[7] Shirina Samreen and Dr. G. Narsimha, "Design of a Novel Trust Model and its application in Trust based Routing to defend against Dishonest Recommenders" in the International Journal of Computer Applications - IJCA, ISSN: 0975 – 8887, Volume 122, No. 2, pp-16-23, July 2015